hoster.by

Доменное имя – источник киберугроз

Наталья Косяк

CLO hoster.by

Фишинг

Малварь и спам

Доменный скам

DNS-атаки (DNS-Flood, DNS spoofing)

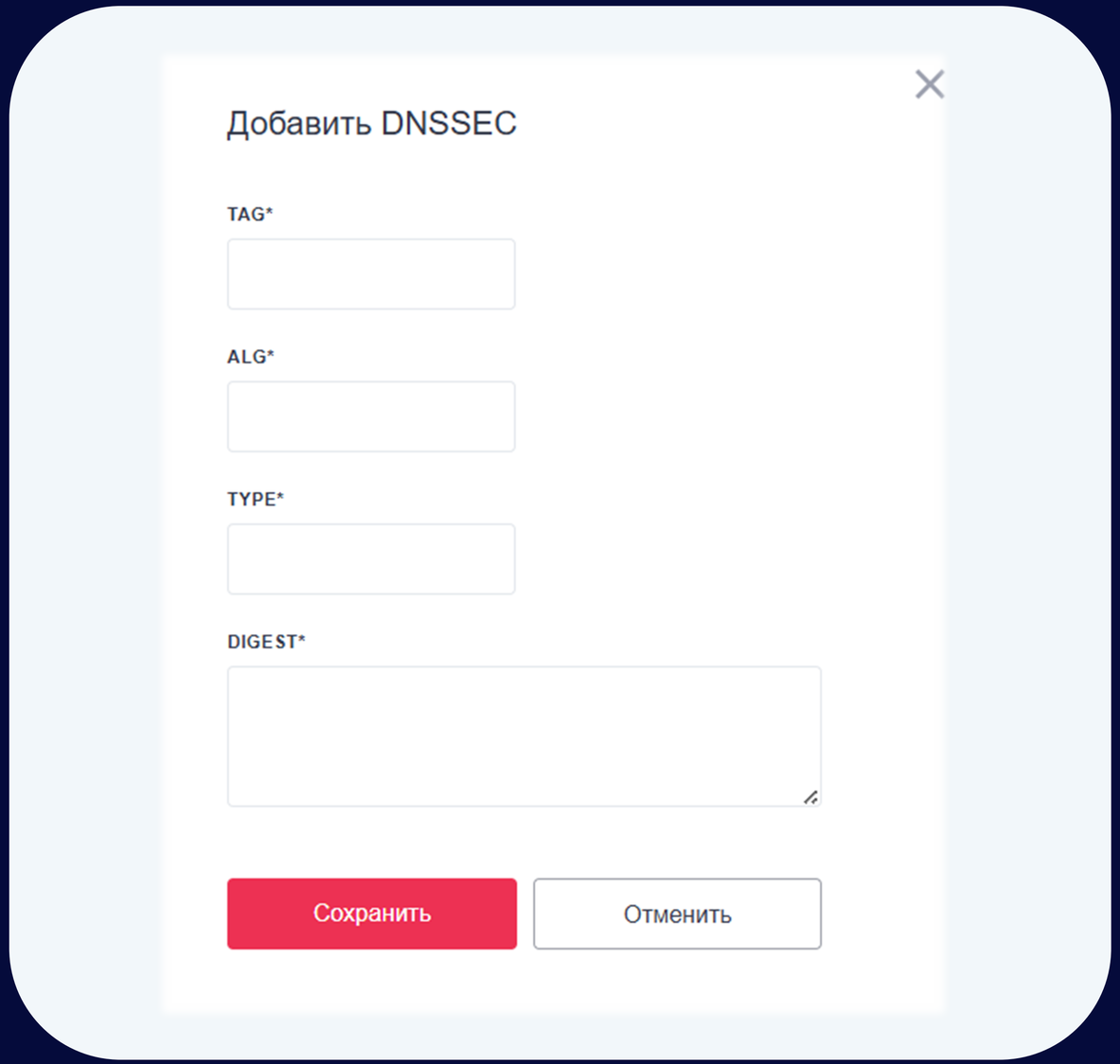
Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

1 **Мониторинг и анализ доменов**

«При выборе доменного имени, в том числе в случае его регистрации по результатам проведения аукциона, заявителю следует избегать названий, тождественных или сходных до степени смешения с наименованиями зарегистрированных средств индивидуализации участников гражданского оборота, товаров (работ, услуг), если заявитель не является обладателем права на фирменное наименование, владельцем товарного знака и знака обслуживания, лицом, обладающим правом пользования географическим указанием.»

Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

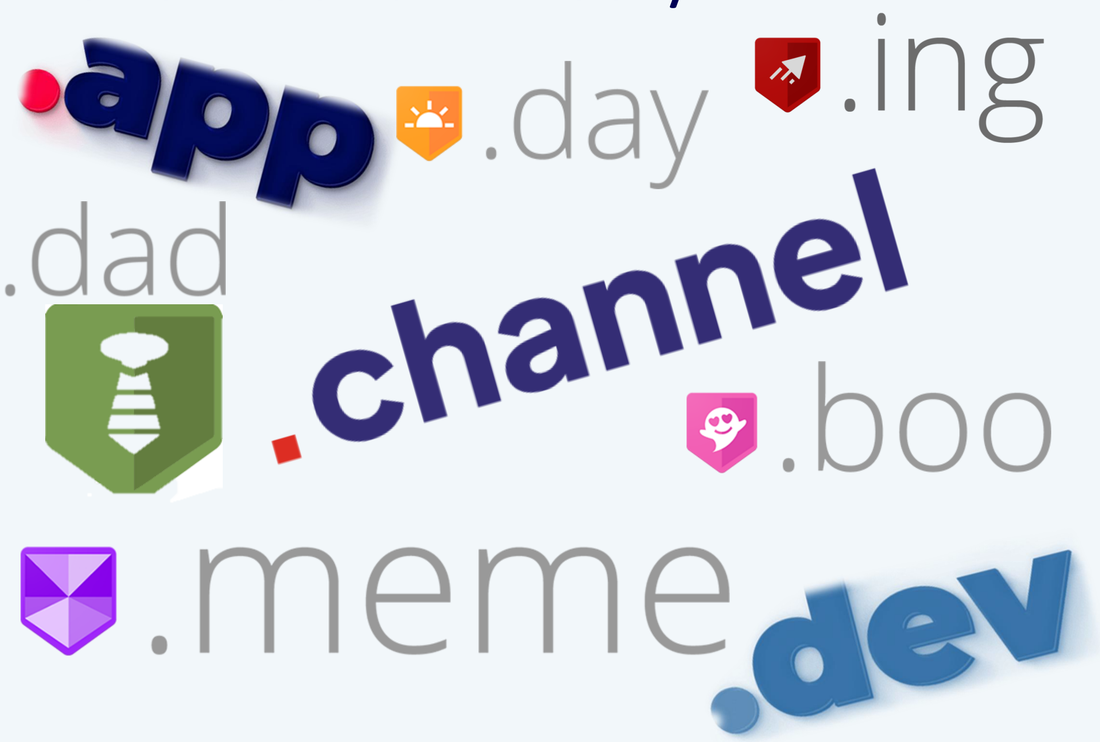
2 **Внедрение DNSSEC**



Методы борьбы со стороны регистраторов регистраторов с киберинцидентами, исходящими от доменных имен

3 **Применение SSL/TLS-сертификатов**

Включение в качестве обязательного требование использования SSL/TLS



Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

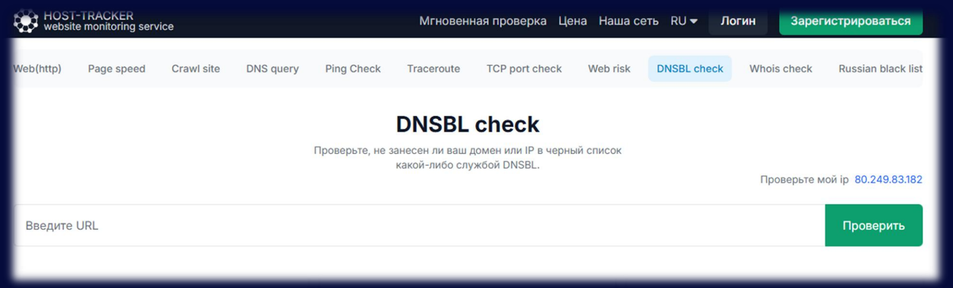
4 **Черные списки (DNSBL, RBL)**

Разработать механизм официального признания DNSBL или тех кто их поддерживает в целях создания единой «инфраструктуры доверия» для формирования возможности использования списков для обмена угрозами. Обязательная публикация критериев внесения в черный список, процедуры исключения из списка, контроль поддержки актуальности данных.

Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

hoster.by

4 **Черные списки (DNSBL, RBL)**

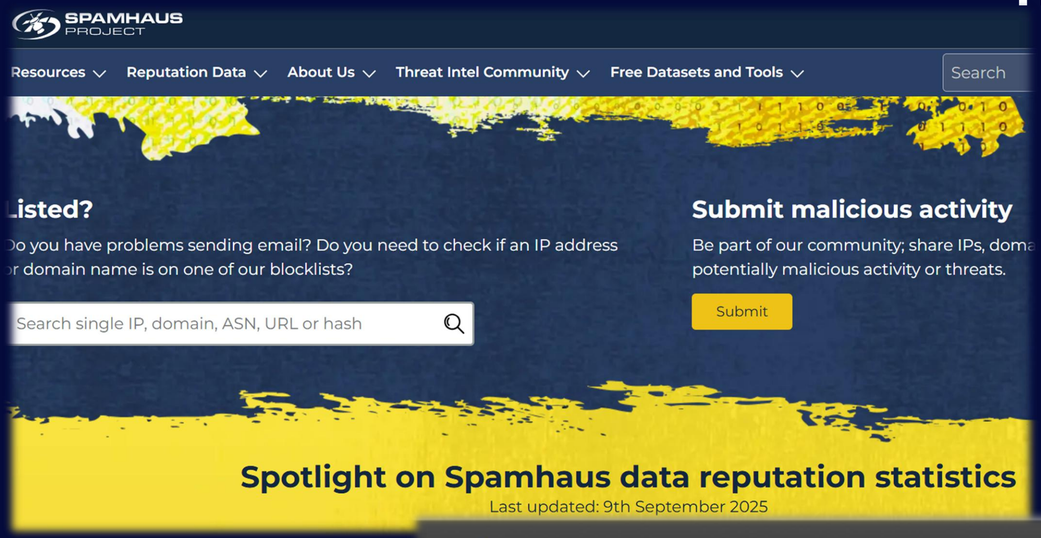


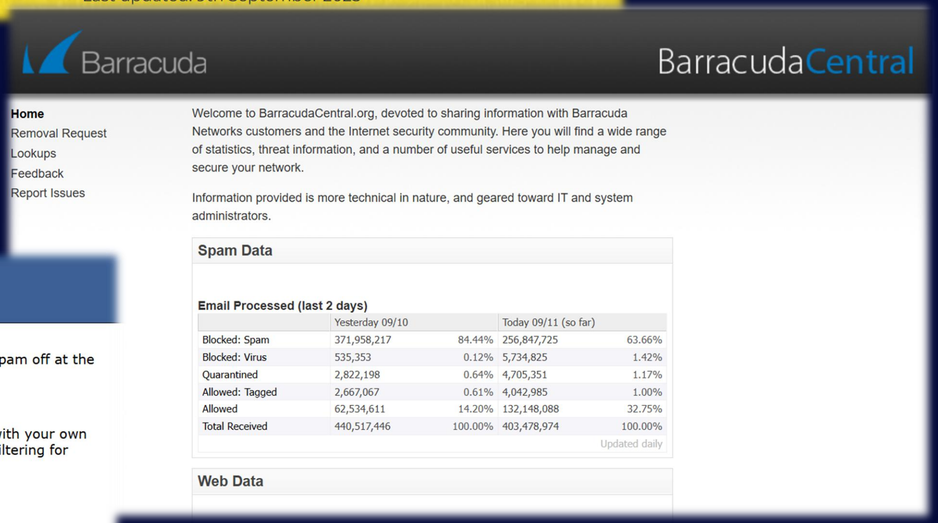
Сформировать требования по единому машиносчитываемому стандарту (на базе JSON/XML) для обмена данными об угрозах между DNSBL-провайдерами, регистраторами и ICANN.

Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

hoster.by

4 **Черные списки (DNSBL, RBL)**





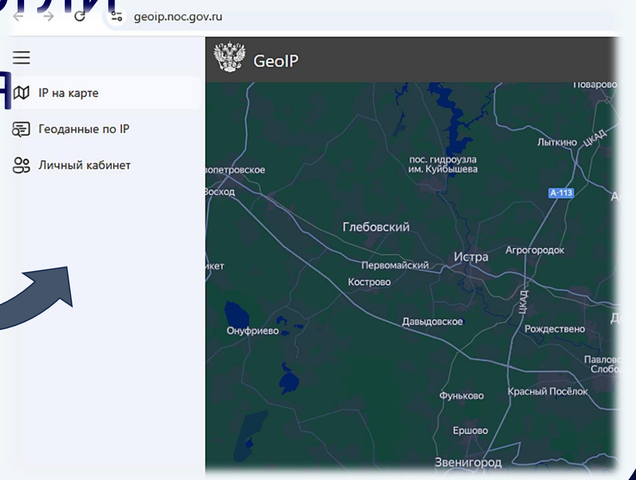
Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

4 **Черные списки (DNSBL, RBL)**

hoster guard

Где используем

К чему не смогли подключиться



Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

5 **Право регистраторов оперативно реагировать**

«Администрирование доменного имени может быть приостановлено:

- *администратором национальной доменной зоны;*
- *судом при рассмотрении дел, связанных с регистрацией и (или) использованием домена;*
- *судебным исполнителем в рамках принятия мер по обеспечению исполнения исполнительного документа (запрещение должнику (владельцу домена) совершать определенные действия).»*

«Делегирование домена может быть приостановлено:

- *на основании требования субъекта профилактики правонарушений (ОВД, прокуратура, органы ГБ, пограничной службы, гос. охраны, финансовых расследований КГК, таможенного органа, органа и подразделения по чрезвычайным ситуациям)»*

Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

6 **Унификация процедур реагирования**

- Создать отдельный, ускоренный внесудебный механизм для изъятия/блокировки доменов, используемых в масштабных кибератаках (ботнеты, DGA, фишинг кампании);
- Решение принимается на основе технических доказательств от аккредитованных субъектов (CERT, SOC);

Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

6 **Унификация процедур реагирования**

- Разработать стандарты предоставления технических доказательств (машинные логи, трафик, образцы вредоносного ПО), которые будут достаточны для быстрого принятия решения об изъятии домена
- Создать единый специальный и безопасный канал для приема заявок на изъятие доменов от доверенных и аккредитованных субъектов. Это исключит необходимость для правоохранительных органов общаться с каждым регистратором по отдельности;

Методы борьбы со стороны регистраторов с киберинцидентами, исходящими от доменных имен

6 **Унификация процедур реагирования**

- Ввести четкие требования в рамках кибербезопасности для регистраторов (наличие SOC, мониторинг аномальной регистрационной активности, реагирование на жалобы в сжатые сроки) как условие сохранения аккредитации;
- Обязанность внедрять системы анализа регистрационной активности для выявления паттернов, характерных для DGA.

Спасибо
за внимание!

Наталья
Косяк

CLO hoster.by

law@hoster.by